GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1473
ANSWERED ON:10.03.2008
HACKING OF WEBSITES
Patil Smt. Rupatai Diliprao Nilangekar

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether a number of cases of hacking of Government Websites especially of the Ministry of Defence have come to the notice of the Union Government;

(b) if so, the details thereof alongwith the names of trie Ministries / Departments whose Websites have been hacked during the last three years, till date;

(c) whether the Government has conducted any official study of the shortcomings in order to ensure cyber security;

(d) if so, the details thereof;

(e) whether the Government has taken any remedial measures in regard to maintaining cyber security in the country; and

(f) if so, the details thereof?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (DR. SHAKEEL AHMAD)

(a) and (b): As per the information tracked by, and reported to Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, a number of Government websites have been hacked during tie period January, 2005 to February, 2008; of which one pertained to a defence related pay office in January, 2006.The websites hacked included those belonging to Ministry of Railways, Air Cargo Customs (Mumbai), Forward markets Commission, National Institute of Health and Family Welfare, National Institute of Social Defence, Dep

(c) to (f): The websi tes were hacked by exploiting technical vulnerabilities in the operating systems, web server, database software and application software.The Government has taken several remedial measures in regard to securing the websites and enhancing the cyber security of information technology infrastructure in the country; these include.

(i) CERT-In has published a Security Guideline for `Securing Websites` and these have been widoly circulated for implementation,

(ii) CERT-In issues security alerts, advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness.

(iii) The organizations operating critical information infrastructure has been advised to implement information security management practices based on International Standard ISO 27001.